**PURPOSE**

To ensure there are appropriate sanctions that will be applied to employees who violate the requirements of the HIPAA Privacy Rule and/or [COVERED ENTITY]’s HIPAA privacy policies and procedures.

**POLICY**

It is [COVERED ENTITY]’s policy to:

* Monitor compliance with HIPAA policies and to mitigate, to the extent practicable, any harm resulting from inappropriate use or disclosure of protected health information.
* Permit individuals to report privacy complaints and issues.
* Impose sanctions, as applicable, for violations of [COVERED ENTITY]’s policies and procedures regarding compliance with HIPAA.

**PROCEDURE**

1. Investigation. When a concern arises regarding a possible violation of HIPAA or [COVERED ENTITY]’s policies or procedures related to HIPAA, the Privacy Official shall begin an investigation promptly.
2. Mitigation. In response to any report of or information about an unauthorized use or disclosure by a member of [COVERED ENTITY]’s workforce or any of its Business Associates, shall develop and implement a plan as soon as reasonably practicable to mitigate any known or reasonably anticipated harmful effects from such disclosure (the :mitigation plan”). The mitigation plan shall be tailored to the circumstances of each case, but shall include as appropriate, the following elements:
   1. Identifying source(s) of the unauthorized use or disclosure and taking appropriate corrective action.
   2. With respect to unauthorized uses of PHI by a member of [COVERED ENTITY]’s workforce, following the Sanction Policy’s process outlined below as applicable.
   3. With respect to unauthorized disclosures of PHI, contacting the recipient of the information that was subject of the unauthorized disclosure and requesting that such recipient either destroy or return the information or take some other appropriate action to mitigate further use or disclosure.
   4. Depending on the circumstances, notifying the patient whose Protected Health Information was the subject of the unauthorized use or disclosure. Depending on the circumstances, notifying the appropriate state and/or federal agency.
3. Sanctions. If, at the conclusion of the investigation, it is found that a violation of [COVERED ENTITY]’s policy or procedure has occurred, the employee involved shall be disciplined in accordance with the severity of the violation and [COVERED ENTITY]’s disciplinary policy. Violations can be classified according to intent such as: (a) those made accidentally or due to a lack of education (Level I Violations); or (b) those made with purposeful disregard of [COVERED ENTITY] policy (Level II Violations).
4. Documentation from the investigation shall be given to the Privacy Officer to be maintained as a part of [COVERED ENTITY]’s HIPAA documentation and retained for six years. The disciplinary action report documenting the employee’s violation shall be placed in the employee’s personnel file as well as a copy provided to the Privacy Officer.

**Guidance for HIPAA Sanctions**

All of [COVERED ENTITY]’s workforce members are accountable for complying with workforce and are accountable for complying with federal and state health information privacy regulations.

The following provides guidance as to how privacy violations will be managed at [COVERED ENTITY]:

1. Review each circumstance of inappropriate use and/or disclosure uniquely and consistently apply corrective disciplinary action. The following considerations may be made when determining the appropriate disciplinary action:
   1. What was the intent of the inappropriate use and/or disclosure?
      1. Unintentional.
      2. Unintentional resulting in a reportable breach.
      3. Intentional.
   2. What is the potential organizational risk associated with the inappropriate use and/or disclosure?
      1. Potential for patient harm.
      2. Potential for organizational harm.
      3. Potential for external/public exposure versus confined internal exposure.
   3. What is the history of the workforce member’s work performance?
      1. Has the member been disciplined for previous patient privacy concerns?
      2. Has the member been subject to a series of progressive disciplinary actions, related or unrelated to patient privacy concerns?
      3. What is the history of the organization’s disciplinary actions for like occurrences?
      4. Are there mitigating circumstances that include conditions that would support reducing the disciplinary/corrective action in the interest of fairness and objectivity?
2. Breaches of PHI or other violations of [COVERED ENTITY]’s HIPAA privacy policies may lead to disciplinary action. Any such violations of [COVERED ENTITY]’s HIPAA policies may also be taken into account in such individual’s performance evaluation. Inappropriate use and/or disclosures of PHI may be divided into the following three levels with recommended corresponding disciplinary action for each. If the workforce member has a history of previous corrective disciplinary actions, then the subsequent disciplinary action should be applied in a progressive manner.

|  |  |  |  |
| --- | --- | --- | --- |
| **LEVEL OF INFRACTION** | **DESCRIPTION OF INFRACTION** | **EXAMPLES OF INFRACTION** | **RANGE OF RECOMMENDED DISCIPLINE** |
| 1 –  Unintentional  Resulting in no  reportable breach | Occurs when member  unintentionally or  carelessly accesses,  reviews or reveals PHI  to him/herself or others  without a legitimate  need to know or beyond  the minimum necessary  level of access assigned  to his/her role. | * Discussion of PHI in public area (cafeterias, elevators of hospital campus). * Typing in wrong MR# or Patient Name and viewing wrong patient’s information. * Leaving PHI accessible within public area (e.g., unattended computer, medical records/surgery schedules in meeting rooms, etc.) | Verbal Reminder and/or additional HIPAA Education |
| 2 –  Unintentional,  Resulting in reportable  breach | Occurs when member  unintentionally or  carelessly accesses,  reviews or reveals PHI  to him/herself or others  without a legitimate  need to know or beyond  the minimum necessary  level of access assigned  to his/her role and such  action results in a  reportable breach. | * Mailing/faxing errors – sending another patient’s documentation to another person/entity resulting in a breach. * Inappropriately accessing/disclosing patient’s medical information (minimum necessary rule not followed, email sensitive information, access to sensitive information outside of role). * Password compromised by sharing it and patient medical information was accessed. * EMR left open and patient medical information was accessed. | Varies depending  on circumstances:  Written reprimand, final warning or unpaid leave.  Severe and multiple  infractions that lead  to breaches may result in  termination pursuant to  applicable [COVERED ENTITY] policies. |
| 3 -  Intentional | Occurs when member  accesses, reviews, or  discusses PHI for  personal gain or with  malicious intent.  Willful and gross  negligent use and/or  disclosure of PHI,  destruction of PHI, or  knowingly violating  state or federal laws  protecting privacy and  security of PHI. | * Inappropriately accessing medical records of family, friends, or prominent people. * Unauthorized and intentional disclosure of patient information to a 3rd party | Varies depending  on circumstances:  Written reprimand,  final warning or unpaid leave.  Severe and multiple  infractions that lead to breaches may result in  termination pursuant to  applicable [COVERED ENTITY] policies. |